What is claimed is:

1. A node in a communications network, comprising:

an identification code;

a control mechanism including configuration information for the node; and

an alarm generator in the control mechanism for raising an alarm to a network user if there is a mismatch between the identification code and the configuration information.

2. The node of claim 1, wherein the identification code is programmed into the backplane of the node.

3. The node of claim 1, further comprising a network protocol based connection, wherein the control mechanism disconnects said connection during the mismatch between the identification code and the configuration information to prevent the configuration information from being downloaded to the node.

4. The node according to claim 1, wherein the node permits live communications traffic to continue uninterrupted through the node during the mismatch.

5. The node according to claim 1, further comprising at least one line card containing hardware elements, wherein said control mechanism is separated from the line card.

6. The node of claim 1, wherein the identification code comprises a chassis serial number.

7. The node of claim 1, wherein the control mechanism is a primary switch management card.

8. The node of claim 7, further comprising a standby switch management card that assumes responsibilities of the primary switch management card in the event of a failure of the primary switch management card.

9. The node of claim 8, wherein the mismatch prevents synchronization of the standby switch management card with the primary switch management card.

10. The node of claim 1, wherein said control mechanism runs a plurality of processes, wherein said processes perform a consistency check between stored configuration information and a hardware configuration for the node.

11. The node of claim 1, further comprising memory for saving a set of default configurations, wherein said node utilizes said set of default configurations when there is a mismatch between the identification code and the configuration information.

12. The node of claim 3, wherein the node disallows trunks from being configured during the mismatch.

13. The node of claim 3, wherein the node disallows circuits from being configured during the mismatch.

14. The node of claim 3, wherein the node prevents improper IP addresses from propagating through the network during the mismatch.

15. A method for restoring configuration information in a node of a communications network, comprising:

performing a consistency check between an identification code programmed into the node and configuration information stored in a control mechanism in the node; and raising an alarm if the consistency check reveals a mismatch between the identification code and the configuration information.

16. The method of claim 15, wherein configuration information is prevented from being downloaded to the node while live communications traffic continues to be processed uninterrupted through the node.

17. The method of claim 15, further comprising a step of preventing invalid IP addresses from propagating through network if there is a mismatch.

18. The method of claim 15, further comprising a step of preventing a set of processes for the node from running if there is a mismatch.

19. A method of preserving configuration information in a node of a communications network when there is a discrepancy between a hardware configuration and configuration information stored in a control mechanism for the node, comprising:

performing a consistency check between the configuration information stored in the control mechanism and the hardware configuration of the node and in the vicinity of the node; and

raising an alarm if said consistency check fails to validate said configuration information against the hardware configuration.

20. The method of claim 19, further comprising a step of identifying inconsistencies between the configuration information and the hardware configuration.

21. The method of claim 19, wherein a port manager raises an alarm if a port configuration is mismatched.

22. The method of claim 19, wherein a trunk manager raises an alarm if a trunk configuration is mismatched.

23. The method of claim 19, wherein a signaling daemon raises an alarm if a cross connect is mismatched.

24. The method of claim 19, further comprising a step of recreating the configuration information in the control mechanism to match the hardware configuration.

25. The method of claim 24, wherein the step of recreating the configuration information in the control mechanism comprises synchronizing the configuration information in the control mechanism with configuration information registered in the hardware of the node.

26. The method of claim 25, wherein the step of recreating the configuration information in the control mechanism further comprises synchronizing the configuration information in the control mechanism with one or more neighboring nodes in the network.